Security Agency, in coordination with the Director, shall perform a study on the use of active defense techniques to enhance the security of agencies, which shall include—

(1) a review of legal restrictions on the use of different active cyber defense techniques in Federal environments, in consultation with the Department of Justice;

(2) an evaluation of—

(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(B) factors that impact the efficacy of the active defense techniques evaluated under subparagraph (A);

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede threat response efforts, criminal investigations, and national security activities, including intelligence collection; and

(4) the development of a framework for the use of different active defense techniques by agencies.

SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operation center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

(b) PLAN.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish a centralized Federal security operations center shared service offering within the Cybersecurity and Infrastructure Security Agency.

(c) CONTENTS.—The plan required under subsection (b) shall include considerations for—

(1) collecting, organizing, and analyzing agency information system data in real time;

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans.

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date on which the plan required under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security operations center as a shared service.

(2) ADDITIONAL AGREEMENTS.—After the date on which the briefing required under subsection (e)(1) is provided, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, may enter into additional 1-year agreements described in paragraph (1) with agencies.

(e) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 260 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).

(2) REPORT.—Not later than 90 days after the date on which the first 1-year agreement entered into under subsection (d) expires, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a report on—

(A) the agreement; and

(B) any additional agreements entered into with agencies under subsection (d).

SA 4675. Mr. SULLIVAN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle E of title VIII, add the following:

SEC. 857. PROHIBITION ON CONTRACTS THAT BENEFIT CHINESE COMMUNIST PARTY.

(a) IN GENERAL.—The Secretary of Defense may not enter into a contract for defense articles or services that are—

(1) developed or manufactured by, or include parts from, the Chinese Communist Party;

(2) provided by an entity that has suspected ties to the Chinese Communist Party; or

(3) provided by an entity that provides defense articles or services, including research, engineering, and technology, to the Chinese Communist Party.

(b) DEFENSE ARTICLES OR SERVICES DEFINED.—In this section, the term ''defense articles or services'' means defense articles or services designated by the President under section 38(a)(1) of the Arms Export Control Act (22 U.S.C. 2778(a)(1)).

SA 4676. Ms. KLOBUCHAR submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in title X, insert the following:

SEC. _____. VETERANS CYBERSECURITY AND DIGITAL LITERACY GRANT PROGRAM.

(a) FINDINGS.—Congress finds the following:

(1) Adversaries from Russia, China, and Iran are using information warfare to influence democracies across the world, and extremist organizations often use digital communications to recruit members. Influence campaigns from foreign adversaries reached tens of millions of voters during the 2016 and 2018 elections with racially and divisively targeted messages. The Unites States can fight these influences by ensuring that citizens of the United States possess the necessary skills to discern disinformation and misinformation and protect themselves from foreign influence campaigns.

(2) Researchers have documented persistent, pervasive, and coordinated online targeting of members of the Armed Forces, veterans, and their families by foreign adversaries seeking to undermine United States democracy in part because of public trust placed in these communities.

(3) A 2017 report by the University of Oxford's Graphika Institute, titled ''Social Media Disinformation Campaigns Against US Military Personnel and Veterans'', concluded that ''The pubic tends to place trust in military personnel and veterans, making them potentially influential voters and community leaders. Given this trust and their role in ensuring national security, these individuals have the potential to become particular targets for influence operations and information campaigns conducted on social media. There are already reports of US service personnel being confronted by foreign intelligence agencies while posted abroad, with details of their personal lives gleaned from social media.''.

(4) The Select Committee on Intelligence of the Senate found in its investigation of the interference in the 2016 election that social media posts by the Internet Research Agency (IRA) of Russia reached tens of millions of voters in 2016 and were meant to pit the people of the United States against one another and sow discord. Volume II of the Committee's investigation found that the Internet Research Agency's Instagram account with the second largest reach used the handle ''@american.veterans'' and was ''aimed at patriotic, conservative audiences, collected 215,680 followers, and generated nearly 18.5 million engagements.''.

(5) A 2019 investigative report by the Vietnam Veterans of America (VVA) titled ''An Investigation into Foreign Entities who are Targeting Troops and Veterans Online'', found that the Internet Research Agency targeted veterans and the followers of several congressionally chartered veterans service organizations with at least 113 advertisements during and following the 2016 election and that ''this represents a fraction of the Russian activity that targeted this community with divisive propaganda.''. The report also found that foreign actors have been impersonating veterans through social-media accounts and interacting with veterans and veterans groups on social media to spread propaganda and disinformation. To counter these acts, Vietnam Veterans of America recommended that the Department of Veterans Affairs ''immediately develop plans to make the cyber-hygiene of veterans an urgent priority within the Department of Veterans Affairs. The VA must educate and train veterans on personal cybersecurity: how to mitigate vulnerabilities, vigilantly maintain safe practices, and recognize threats, including how to identify instances of online manipulation.''.

(6) The Cyberspace Solarium Commission, a bicameral and bipartisan commission, established by section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232), concluded in its finished report that the ''U.S. government should promote digital literacy, civics education, and public awareness to build societal resilience to foreign, malign cyber-enabled information operations and that the U.S. government must ensure that individual Americans have both the digital literacy tools and the civics education they need to secure their networks and their democracy from cyber-enabled information operations.''. The report recommended that Congress authorizing grant programs to do this.

(b) SENSE OF CONGRESS.—It is the sense of Congress that, given the threat foreign influence campaigns pose for United States democracy and the findings and recommendations of Congress and experts, Congress must immediately act to pass legislative measures